LISTING OF THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application. Where claims have been amended and/or canceled, such amendments and/or cancellations are done without prejudice and/or waiver and/or disclaimer, and the right to claim this subject matter in a continuing application is hereby reserved.

1. (Previously presented) In an apparatus, a method of operation comprising: generating in real time a first deciphering round key based on a deciphering key;

incrementally deciphering a ciphered text for a first round using the real time generated first deciphering round key to generate a partially deciphered text;

generating in real time a second deciphering round key based, at least in part, on said generated first deciphering round key while said incremental deciphering for said first round is being performed; and

incrementally deciphering the partially deciphered text for a second round using the real time generated second deciphering round key.

2. (Original) The method of claim 1, wherein said first and second deciphering round keys comprise first and second plurality of round key data words respectively, and said generation in real time of said second deciphering round keys comprises iteratively generating said second plurality of round key data words over a plurality of iterations.

3. (Currently amended) The method of claim 2, wherein said iterative generation of said second plurality of round key data words over a plurality of iterations comprises generating one of said second plurality of round key data words during each iteration, including performing ~~performance of~~ a first XOR operation on a first and a second round key data word during each iteration.

4. (Previously presented) The method of claim 3, wherein said first round key data word employed in said first XOR operation during each iteration is a first predecessor round key data word of one deciphering master key length preceding said one of the second plurality of

the round key data words to be generated, and said second round key data word employed is a conditionally transformed second predecessor round key data word immediately following the first predecessor round key data word.

5. (Original) The method of claim 4, wherein said second round key data word employed is an untransformed version of said second predecessor round key data word.

6. (Original) The method of claim 4, wherein said second round key data word employed is a substitution value looked up from a substitution box using an inverse of said second predecessor round key data word.

7. (Currently amended) The method of claim 4, wherein said second round key data word employed is a thrice transformed version of said second predecessor round key data word generated by performing a second XOR operation on a twice transformed version of said second predecessor round key data word and a value that is functionally dependent on an iteration index value.

8. (Currently amended) The method of claim 7, wherein said twice transformed version of said second predecessor round key data word is a value looked up from a substitution box using an inverse of a[[n]] once transformed version of said second predecessor round key data word.

9. (Currently amended) The method of claim 8, wherein ~~for~~ said once transformed version of said second predecessor round key data word is generated by rotationally shifting said second predecessor round key data word in a predetermined shifting direction for a predetermined shifting amount.

10. (Currently amended) An apparatus comprising:

a deciphering round key generator to successively generate in real time at least a first and a second deciphering round key based on a deciphering key; and

a deciphering unit coupled to the deciphering round key generator to successively employ said real time successively generated deciphering round keys to incrementally decipher a ciphered text,[[;]]

wherein said deciphering round key generator at least generates said second deciphering round key in real time while said deciphering unit deciphers said ciphered text employing said real time generated first deciphering round key.

11. (Original) The apparatus of claim 10, wherein said first and second deciphering round keys comprise first and second plurality of round key data words respectively, and said deciphering round key generator generates said second deciphering round keys in real time by iteratively generating said second plurality of round key data words over a plurality of iterations.

12. (Currently amended) The apparatus of claim 11, wherein said deciphering round key generator comprises a first XOR function, and iteratively generates said second plurality of round key data words over a plurality of iterations by generating one of said second plurality of round key data words during each iteration, performing an XOR operation on a first and a second round key data word using said first XOR function.

13. (Previously presented) The apparatus of claim 12, wherein said first round key data word employed in each iteration is a first predecessor round key data word of one deciphering master key length preceding said one of the second plurality of the round key data words to be generated, and said second round key data word is a conditionally transformed second predecessor round key data word immediately following said first predecessor round key data word.

14. (Currently amended) The apparatus of claim 13, wherein said deciphering round key generator further comprises conditional passthru circuitry and transformation circuitry coupled to said first XOR function in parallel to provide said XOR function with an untransformed version or a[[n]] one or more times transformed version of said predecessor round key data word, depending on at least multiplicity between an iteration index value and a deciphering master key length.

15. (Original) The apparatus of claim 14, wherein said deciphering round key generator further comprises a substitution box and an inverse lookup circuitry serially coupled to said passthru circuitry to substitute the second predecessor round key data word with a substitute value looked up using an inverse of said second predecessor round key data word.

16. (Currently amended) The apparatus of claim 14, wherein said deciphering round key generator further comprises a second XOR function coupled to said passthru circuitry to perform a second XOR operation on an at least a once transformed version of said second predecessor round key data word and a value that is functionally dependent on an iteration index value.

17. (Currently amended) The apparatus of claim 16, wherein said deciphering round key generator further comprises a lookup table coupled to said second XOR function and having stored therein said functionally dependent values to be looked up using a value that depends on a deciphering master key length and an amount of iteration performed.

18. (Currently amended) The apparatus of claim 16, wherein said deciphering round key generator further comprises a substitution box and inverse lookup circuitry serially coupled to said second XOR function to provide the second XOR function with said at least once transformed version of said second predecessor round key data word, generated by substituting an inverse of an least once transformed version of said second predecessor round key data word with a substitute value.[[,]]

19. (Original) The apparatus of claim 18, wherein said deciphering round key generator further comprises a rotational shifter coupled to said inverse lookup circuitry to provide said inverse lookup circuitry with said at least once transformed version of said second predecessor round key data word, generated by rotationally shifting the said second predecessor round key data word.

20. (Currently amended) The apparatus of claim 10, wherein said apparatus is disposed

on an integrated ~~integ rated~~ circuit.

21. (Currently amended) A routing apparatus comprising:

a first deciphering round key generator to successively generate in real time at least a first and a second deciphering round key based, at least in part, on a first deciphering key for a first network traffic flow;

a first deciphering unit coupled to the first deciphering round key generator to successively employ said real time successively generated at least first and second deciphering round keys to incrementally decipher a first ciphered text for the first network traffic flow;

a second deciphering round key generator to successively generate in real time at least a third and a fourth deciphering round key based, at least in part, on a second deciphering key for a second network traffic flow; and

a second deciphering unit coupled to the second deciphering round key generator to successively employ said real time successively generated at least third and fourth deciphering round keys to incrementally decipher a second ciphered text for the second network traffic flow,[[;]]

wherein said first deciphering round key generator at least generates said second deciphering round key in real time while said first deciphering unit deciphers said first ciphered text employing said real time generated first deciphering round key, and said second deciphering round key generator at least generates said fourth deciphering round key in real time while said second deciphering unit deciphers said second ciphered text employing said real time generated third deciphering round key.

22. (Currently amended) The routing apparatus of claim 21, wherein said first, second, third and fourth deciphering round keys comprise first, second, third and fourth plurality of round key data words respectively, and said first and second deciphering round key generator generate said second and fourth deciphering round keys in real time by iteratively generating said second and fourth plurality of round key data words over a first and a second plurality of iterations, respectively.

23. (Currently amended) The routing apparatus of claim 22, wherein each of said first/second deciphering round key generator comprises a first XOR function, and iteratively generates said second/fourth plurality of round key data words over a plurality of iterations, respectively, by generating one of said second/fourth plurality round key data words during each iteration, performing an XOR operation on a first and a second round key data word using said first XOR function.

24. (Previously presented) The routing apparatus of claim 23, wherein said first round key data word employed in each iteration is a first predecessor round key data word of said second/fourth plurality of round key data words of one deciphering master key length preceding said one of the second/fourth plurality of the round key data words to be generated, and said second round key data word employed is a conditionally transformed second predecessor round key data word immediately following the first predecessor round key data word.

25. (Currently amended) The routing apparatus of claim 23, wherein each of said first/second deciphering round key generators further comprises conditional passthru circuitry and transformation circuitry coupled to said first XOR function in parallel to provide said XOR function with an untransformed version or a[[n]] one or[[e]] more times transformed version of said second predecessor round key data word depending on at least multiplicity between an iteration index value and a deciphering master key length.

26. (Currently amended) The routing apparatus of claim 25, wherein each of said first/second deciphering round key generators further comprises a substitution box and an inverse lookup circuitry serially coupled to said passthru circuitry to substitute the second predecessor round key data word with a substitute value looked up using an inverse of said second predecessor round key data word.

27. (Currently amended) The routing apparatus of claim 25, wherein each of said first/second deciphering round key generators further comprises a second XOR function coupled to said passthru circuitry to perform a second XOR operation on an at least once

transformed version of said second predecessor round key data word and a value that is functionally dependent on an iteration index value.

28. (Currently amended) The routing apparatus of claim 27, wherein each of said first/second deciphering round key generators further comprises a lookup table coupled to said second XOR function and having stored therein said functional dependent values to be looked up using a value that depends on a deciphering master key length and an amount of iteration performed.

29. (Currently amended) The routing apparatus of claim 27, wherein each of said first/second deciphering round key generators further comprises a substitution box and inverse lookup circuitry serially coupled to said second XOR function to provide the second XOR function with said at least once transformed version of said second predecessor round key data word, generated by substituting an inverse of an at least once transformed version of said second predecessor round key data word with a substitute value.

30. (Currently amended) The routing apparatus of claim 29, wherein each of said first/second deciphering round key generators further comprises a rotational shifter coupled to said inverse lookup circuitry to provide said inverse lookup circuitry with said at least once transformed version of said second predecessor round key data word, generated by rotationally shifting said second predecessor round key data word.

31. (Original) The routing apparatus of claim 21, wherein said routing apparatus is disposed on an integrated circuit.